

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-171887

(43) 公開日 平成10年(1998) 6月26日

(51) Int.Cl.⁶

G 0 6 F 17/60

識別記号

F I

G 0 6 F 15/21

3 3 0

3 4 0 Z

審査請求 未請求 請求項の数13 O L (全 17 頁)

(21) 出願番号

特願平8-333387

(22) 出願日

平成8年(1996)12月13日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 広谷 政彰

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72) 発明者 千葉 寛之

神奈川県横浜市都筑区加賀原二丁目2番

株式会社日立製作所ビジネスシステム開発

センタ内

(74) 代理人 弁理士 小川 勝男

最終頁に続く

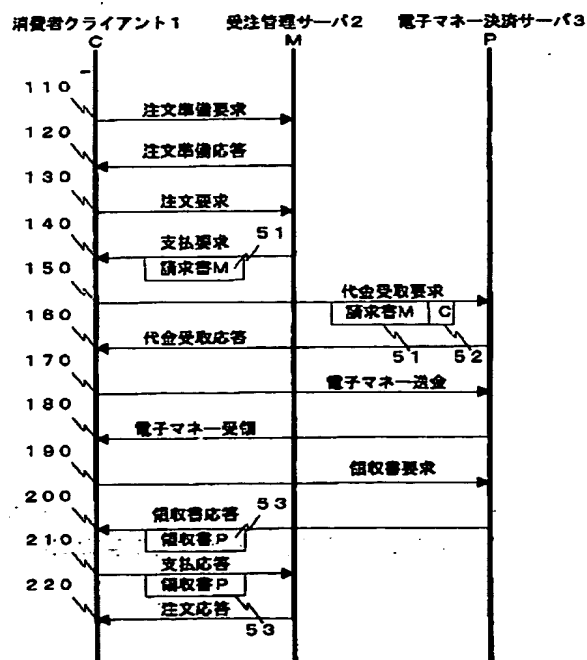
(54) 【発明の名称】 オンラインショッピングシステム

(57) 【要約】

【課題】 電子マネーを利用して取引する場合に、取引内容や決済が完了したことを客観的に証明できる電子データをオープンネットワーク上で提供する。

【解決手段】 購入プロセスでは、受注管理サーバに請求書データを発行する手段と、電子マネー決済サーバに領収書データを発行する手段を設け、消費者クライアントは発注し、受注管理サーバから請求書データを受信し、データを電子マネー決済サーバに送信後、電子マネーを送信し電子マネー決済サーバから受信して領収書データを受注管理サーバに送信して取引が完了する。払戻プロセスでは、受注管理サーバに払戻許可書データを発行する手段と、消費者クライアントに払戻領収書を発行する手段を設け、消費者クライアントが払戻許可書を受信すると、データを電子マネー決済サーバに送信し、電子マネー決済サーバから電子マネーを受領し、電子マネー決済サーバに払戻領収書データを送信し払戻が完了する。

図5



【特許請求の範囲】

【請求項1】複数の情報処理装置がネットワークで相互に接続されているコンピュータシステムにおいて、第1の情報処理装置は、注文データなどを入力するための手段と、注文データと請求書データと領収書データを表示するための手段と、注文データを送信するための手段と、請求書データと領収書データを送受信するための手段と、電子マネーを格納するための手段と、電子マネーを送受信するための手段を有し、第2の情報処理装置は前記注文データを受信するための手段と、前記注文データを記憶するための手段と、少なくとも支払先である第3の情報処理装置を特定するためのデータと取引を特定するための識別子と支払金額で構成されるデータに前記第2の情報処理装置が有する秘密鍵で暗号化したデジタル署名を添付した請求書データを発行するための手段と、前記請求書データを送信するための手段と、領収書データを受信する手段と、前記領収書データに添付されているデジタル署名が前記請求書データで指定した支払先が有する秘密鍵でデジタル署名されたものかどうかをチェックするための手段を有し、第3の情報処理装置は、電子マネーを格納する手段と、電子マネーを送受信するための手段と、決済データを記憶するための手段と、少なくとも領収金額と取引を特定するための識別子で構成されるデータに第3の情報処理装置が有する秘密鍵で暗号化したデジタル署名を添付した領収書データを発行する手段と、前記領収書データを送信するための手段を有することを特徴とするオンラインショッピングシステム。

【請求項2】請求項1記載のオンラインショッピングシステムにおいて、前記第1の情報処理装置が前記第2の情報処理装置に注文データを送信するステップと、前記第2の情報処理装置が前記注文データを受信した場合に前記請求書データを発行して前記第1の情報処理装置に送信するステップと、前記第1の情報処理装置が前記請求書データを受信すると前記第3の情報処理装置に前記請求書データを送信するステップと、前記第3の情報処理装置の応答に対して前記第1の情報処理装置から前記第3の情報処理装置に電子マネーを送金するステップと、前記第3の情報処理装置が前記電子マネーを受信したら前記領収書データを発行して前記第1の情報処理装置に送信するステップと、前記第1の情報処理装置が前記領収書データを受信したら、前記領収書データを前記第2の情報処理装置に送信するステップを有することを特徴とするオンラインショッピングシステム。

【請求項3】請求項2記載のオンラインショッピングシステムにおいて、前記第1の情報処理装置が前記第3の情報処理装置に請求書データを送信するステップの前に、前記請求書データを含む前記ステップで送信するデータに前記第1の情報処理装置が有する秘密鍵で暗号化したデジタル署名を添付するステップを追加することを

特徴とするオンラインショッピングシステム。

【請求項4】複数の情報処理装置がネットワークで相互に接続されているコンピュータシステムにおいて、第1の情報処理装置は注文データなどを入力するための手段と、注文データと請求書データと領収書データを表示するための手段と、電子マネーを格納するための手段と、電子マネーを送受信するための手段と、注文データを送信するための手段と、請求書データと領収書データを送受信する手段を有し、かつ前記第1の情報処理装置は、第2の情報処理装置に注文データを送信するステップと、前記第2の情報処理装置から請求書データを受信すると第3の情報処理装置に前記請求書データを送信するステップと、前記第3の情報処理装置からの応答に応じて前記第3の情報処理装置へ電子マネーを送信するステップと、前記第3の情報処理装置から領収書データを受信すると前記領収書データを前記第2の情報処理装置に送信するステップを有することを特徴とするオンラインショッピングシステム。

【請求項5】複数の情報処理装置がネットワークで相互に接続されているコンピュータシステムにおいて、第2の情報処理装置は、注文データを受信する手段と、前記注文データを記憶するための手段と、少なくとも支払先を特定するためのデータと取引を特定するための識別子と支払金額で構成されるデータに前記第2の情報処理装置が有する秘密鍵で暗号化したデジタル署名を添付した請求書データを発行する手段と、前記請求書データを送信するための手段と、領収書データを受信するための手段と、前記領収書データに添付されているデジタル署名が前記請求書データで指定した支払先が有する秘密鍵によってデジタル署名されたものかどうかをチェックするための手段を有し、第2の情報処理装置は、第1の情報処理装置から注文データを受信した場合に前記請求書データを発行するステップと前記請求書データを前記第1の情報処理装置に送信するステップを有し、さらに領収書データを受信した場合に前記領収書データが前記請求書データで指定した支払先によってデジタル署名されたものであることを判断するステップを有することを特徴とするオンラインショッピングシステム。

【請求項6】複数の情報処理装置がネットワークで相互に接続されているコンピュータシステムにおいて、第3の情報処理装置は、請求書データを受信するための手段と、決済データを記憶するための手段と、少なくとも領収金額と取引を特定するための識別子で構成されるデータに前記第3の情報処理装置が有する秘密鍵で暗号化したデジタル署名を添付した領収書データを発行する手段と、電子マネーを格納するための手段と、電子マネーを送受信するための手段を有し、前記第3の情報処理装置は、第2の情報処理装置が発行した請求書データを第1の情報処理装置から受信するステップと、前記請求書データの有効性をチェックするステップと、前記請求書

データが有効である場合に前記第1の情報処理装置に送金許可を送信するステップと、前記第1の情報処理装置から電子マネーを受信したら領収書データを発行するステップと、前記領収書データを前記第1の情報処理装置に送信するステップを有することを特徴とするオンラインショッピングシステム。

【請求項7】複数の情報処理装置がネットワークで相互に接続されているコンピュータシステムにおいて、第1の情報処理装置は、少なくとも取引を特定するためのデータを含む払戻要求を送信する手段と、電子マネーを格納するための手段と、電子マネーを送受信するための手段と、少なくとも取引を特定するための識別子と受領した払戻金額に関するデータで構成されるデータにデジタル署名を添付した払戻領収書を発行するための手段と、前記払戻領収書を送信するための手段と、払戻許可データを送受信するための手段を有し、第2の情報処理装置は、前記払戻要求を受信するための手段と、注文データを記憶するための手段と、少なくとも払戻を行う第3の情報処理装置を特定するためのデータと払戻金額に関するデータと払戻を受領する人もしくは払戻を受領する第1の情報処理装置を特定するためのデータで構成されるデータにデジタル署名を添付した払戻許可データを発行するための手段と、前記払戻データを送信するための手段を有し、第3の情報処理装置は、前記払戻許可データを受信するための手段と、前記払戻許可データの有効性をチェックするための手段と、電子マネーを格納するための手段と、電子マネーを送受信するための手段と、決済データを記憶するための手段を有することを特徴とするオンラインショッピングシステム。

【請求項8】請求項7記載の払戻領収書の払戻を受領する人もしくは払戻を受領する第1の情報処理装置を特定するためのデータが、デジタル署名の正当性を証明するために使用される認証局に登録されている証書データに含まれる人もしくは情報処理装置を特定するためのデータであることを特徴とするオンラインショッピングシステム。

【請求項9】請求項7記載のオンラインショッピングシステムにおいて、前記第1の情報処理装置が前記第2の情報処理装置に払戻要求を送信するステップと、前記第2の情報処理装置が前記払戻要求を受信した場合に前記払戻許可データを発行して前記第1の情報処理装置に送信するステップと、前記第1の情報処理装置が前記払戻許可データを受信すると前記第3の情報処理装置に前記払戻許可データを送信するステップと、前記払戻許可データが有効である場合に前記第3の情報処理装置から前記第1の情報処理装置に電子マネーを送金するステップと、前記第1の情報処理装置が前記電子マネーを受信したら前記第3の情報処理装置に払戻領収書データを送信するステップを有することを特徴とするオンラインショッピングシステム。

【請求項10】請求項9記載のオンラインショッピングシステムにおいて、前記第1の情報処理装置が前記第3の情報処理装置に前記払戻許可データを送信するステップの前に、前記払戻許可データを含む前記ステップで送信するデータに前記第1の情報処理装置が有する秘密鍵で暗号化したデジタル署名を添付するステップを追加することを特徴とするオンラインショッピングシステム。

【請求項11】複数の情報処理装置がネットワークで相互に接続されているコンピュータシステムにおいて、第1の情報処理装置は、少なくとも取引を特定するためのデータを含む払戻要求を送信する手段と、電子マネーを格納するための手段と、電子マネーを送受信する手段と、少なくとも取引を特定するための識別子と受領した払戻金額に関するデータで構成されるデータにデジタル署名を添付した払戻領収書を発行するための手段と、前記払戻領収書を送信するための手段と、払戻許可データを送受信するための手段を有し、前記第1の情報処理装置は、払戻要求を送信するステップと、第2の情報処理装置から前記払戻許可データを受信した場合に、前記払戻許可データに前記第1の情報処理装置が有する秘密鍵で暗号化したデジタル署名を添付して第3の情報処理装置に送信するステップと、前記第3の情報処理装置から電子マネーを受信するステップと、前記電子マネーを受信した場合に払戻領収書データを発行するステップと、前記払戻領収書を前記第3の情報処理装置に送信するステップを有することを特徴とするオンラインショッピングシステム。

【請求項12】複数の情報処理装置がネットワークで相互に接続されているコンピュータシステムにおいて、第2の情報処理装置は、前記払戻要求を受信するための手段と、注文データを記憶するための手段と、少なくとも払戻を行う第3の情報処理装置を特定するためのデータと払戻金額に関するデータと払戻を受領する人もしくは払戻を受領する第1の情報処理装置を特定するためのデータで構成されるデータにデジタル署名を添付した払戻許可データを発行する手段と、前記払戻データを送信するための手段を有し、第2の情報処理装置は、第1の情報処理装置から払戻要求を受信した場合に前記払戻許可データを発行するステップと前記払戻許可データを前記第1の情報処理装置に送信するステップと、前記第3の情報処理装置に払戻完了状態を問い合わせるステップを有することを特徴とするオンラインショッピングシステム。

【請求項13】複数の情報処理装置がネットワークで相互に接続されているコンピュータシステムにおいて、第3の情報処理装置は、前記払戻許可データを受信するための手段と、前記払戻許可データの有効性をチェックするための手段と、電子マネーを格納するための手段と、電子マネーを送受信するための手段と、決済データを記憶するための手段を有し、前記第3の情報処理装置は、

第2の情報処理装置が発行した払戻許可データを第1の情報処理装置から受信するステップと、前記払戻許可データの有効性をチェックするステップと、前記払戻許可データが有効である場合に前記第1の情報処理装置に電子マネーを送信するステップと、前記第1の情報処理装置から払戻領収書データを受信するステップと、前記第2の情報処理装置から払戻完了状態の問合せがあった場合に、前記第2の情報処理装置に払戻完了状態を送信するステップを有することを特徴とするオンラインショッピングシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 インタネットなどのオープンなネットワークで電子マネーを利用して安全に取引するためのシステムに関する

【0002】

【従来の技術】 現在、インタネットなどのオープンなネットワークを使用してショッピングを行なうシステムが台頭してきている。既存のシステムでは、小売店はWWW(World Wide Web)サーバで商品情報を消費者に提供し、消費者はWWWブラウザで商品情報を見て購入したい商品を選択し、注文を出している。決済手段としては、クレジットカードを使用する方法と電子マネーを使用する方法が主流である。インタネットショッピングで問題になるのはセキュリティである。インタネットは誰でも簡単にアクセスできるために、第三者によって盗聴されたり、改ざんされる可能性がある。また第三者が成りすまして取引を行なう可能性もある。また取引に関与する当事者がデータを改ざんしたり、取引内容を否定したり、代金を持ち逃げしたりする可能性がある。既存のシステムでは、これらの問題に対応するために、データの暗号化、デジタル署名、認証局などを利用している。データの暗号化方式には、DES(DataEncryption Standard)やRSAなどがある。これらの技術を利用した代表的なプロトコルとして、VISA社とMasterCard社が開発したクレジットカード決済を対象としたセキュア電子取引プロトコル(SET)がある。暗号化方式、デジタル署名方式、認証局方式については、SETの仕様書に記載されている。また電子マネーシステムとしては、Digicash社のecash、Mondex社のMondexマネーなどがある。Mondex社の基本特許として特表平5-504643がある。

【0003】

【発明が解決しようとする課題】 既存のオープンネットワーク対応のショッピングシステムや、電子マネーシステムでは、通信中のデータの盗聴や改ざんを防止するために、暗号化やデジタル署名を利用している。SETはクレジットカード決済を前提とした取引プロトコルであり、オープンネットワーク上では小売店に対する発注処理とカード会社に対する承認処理だけを行ない、決済処

理は既存の金融ネットワークで行なっている。この場合、取引内容を証明する請求書はカード所有者に郵送され、決済が完了したことは、銀行口座からの引き落とし記録で立証できる。オープンネットワーク上で電子マネーを利用して取引する場合には、基本的に全ての処理は決済処理も含め、オープンネットワーク上で実行される。そこで取引内容や決済が完了したことを客観的に証明できる電子データをオープンネットワーク上で提供する必要がある。これらのデータは、通信途中で第三者によって書き換えられては困るし、またそれらのデータを受取った取引当事者によって自分の都合のよいように勝手に書き換えられても困る。また信用を有する第三者機関が決済の代行を行なう場合、注文を行う情報処理装置(発注クライアント)と、注文を受けつけたり注文を管理する情報処理装置(注文管理サーバ)と、代金を受領して管理する情報処理装置(決済サーバ)がそれぞれ独立にネットワークに接続される。この場合、注文情報や決済情報が改ざんされることなくこれらの情報処理装置間で転送され、かつ後日何か問題が発生した場合には、取引関係者がこれらの注文情報や決済情報を提示することで注文内容や決済完了を確認できたり、それらが改ざんされていないことを証明できる手段が必要である。さらに商品を購入する場合のみならず、商品を返品したり取引をキャンセルした場合に、オープンネットワーク上で電子マネーを使用して購入者に代金を払い戻せる必要がある。この場合、第三者が不正に払戻金を受け取ることがないようにする必要がある。本発明の目的は、オープンネットワーク上で電子マネーを使用してショッピングを行う場合に、ネットワーク上で取引内容や決済状態を証明するデータを取引関係者に提供する手段を提供することにある。本発明の別の目的は、注文する情報処理装置と、注文を受けつけ管理する情報処理装置と、代金を受領および管理する情報処理装置が独立にネットワークに接続されている場合に、取引上のトラブルを回避する手段を提供することにある。さらに本発明の別の目的は、オープンネットワーク上で電子マネーを使用して購入者に代金を払い戻す場合に、不正に第三者によって払戻金を横取りされずに、正規の購入者に払い戻す手段を提供することにある。

【0004】

【課題を解決するための手段】 上記目的を達成するために、複数の情報処理装置がネットワークで相互に接続されているコンピュータシステムにおいて、発注を行う第1の情報処理装置に電子マネーを送受信する手段と、注文データを送信するための手段と、請求書データや領収書データを送受信する手段を設け、注文を受け付け、管理する第2の情報処理装置に注文データを受信するための手段と、注文データを記憶するための手段と、少なくとも支払金額と支払先と取引を特定するための識別子を含むデータに第2の情報処理装置が有する秘密鍵で暗号

化したデジタル署名を添付した請求書データを発行するための手段と、請求書データを送信するための手段と、支払先のデジタル署名が添付された領収書データを受信して領収書の有効性をチェックするための手段を設け、代金を受領・管理する第3の情報処理装置に電子マネーを送受信するための手段と、決済データを記憶するための手段と、少なくとも領収金額と取引を特定するための識別子を含むデータに第3の情報処理装置が有する秘密鍵で暗号化したデジタル署名を添付した領収書データを発行する手段と、領収書データを送信するための手段を設ける。請求書データと領収書データには、発行者のみが有する秘密鍵で暗号化されたデジタル署名が添付されているので、発行者以外が改造することは困難であり、商品購入者がこれらのデータを提示すれば、取引内容やその取引の決済が完了したなどを証明できる。さらに第1の情報処理装置が第2の情報処理装置に注文データを送信するステップと、第2の情報処理装置が注文データを受信した場合に第1の情報処理装置に請求書データを送信するステップと、第1の情報処理装置が請求書データを受信すると第3の情報処理装置に請求書データを送信するステップと、第3の情報処理装置の応答に対して第1の情報処理装置から第3の情報処理装置に電子マネーを送金するステップと、第3の情報処理装置が電子マネーを受信したら第1の情報処理装置に領収書を送信するステップと、第1の情報処理装置が領収書を受信したら、領収書を第2の情報処理装置に送信するステップを設ける。このことにより、発注のための第1の情報処理装置と、受注のための第2の情報処理装置と、代金を受領する第3の情報処理装置がそれぞれオープンネットワークに接続されている場合であっても、問題が発生した場合にその問題の所在を明確にすることが可能になる。また代金の払戻を行なうために、第1の情報処理装置に払戻要求を送信するための手段と、電子マネーを送受信する手段と、少なくとも取引を特定するための識別子と受領した払戻金額に関するデータで構成されるデータに第1の情報処理装置が有する秘密鍵で暗号化したデジタル署名を添付した払戻領収書を送信するための手段と、払戻許可データを発行するための手段と、払戻許可データを発行するための手段を設け、第2の情報処理装置に、払戻要求を受信するための手段と、注文データを記憶するための手段と、少なくとも取引を特定するための識別子と払戻金の受取人を特定するための識別子と払戻金額に関する情報を含むデータに第2の情報処理装置が有する秘密鍵で暗号化したデジタル署名を添付した払戻許可書データを発行するための手段と、払戻許可書データを送信するための手段を設け、第3の情報処理装置に、払戻許可書データを受信するための手段と、前記払戻許可書データの有効性をチェックするための手段と、電子マネーを格納するための手段と、電子マネーを送受信するための手段と、決済データを記憶するための手段を設

ける。さらにオンラインショッピングシステムにおいて、第1の情報処理装置が第2の情報処理装置に払戻要求を送信するステップと、第2の情報処理装置が前記払戻要求を受信した場合に払戻許可データを発行して第1の情報処理装置に送信するステップと、第1の情報処理装置が払戻許可データを受信すると第3の情報処理装置に払戻許可データを送信するステップと、払戻許可データが有効である場合に第3の情報処理装置から第1の情報処理装置に電子マネーを送金するステップと、第1の情報処理装置が電子マネーを受信したら第3の情報処理装置に払戻領収書データを送信するステップを設ける。以上により、払戻を要求する情報処理装置と、注文データを管理していて払戻を受け付ける情報処理装置と、払戻金を送金する電子マネー決済サーバがそれぞれネットワークに接続されている場合であっても、正当な払戻受領者に払戻金を送金することが可能になるとともに、払戻金の受領に関してトラブルが発生した場合には、払戻許可データや払戻領収書データを提示することにより問題を解決することが可能になる。払戻許可データと払戻領収書データには、発行者のみが有する秘密鍵で暗号化されたデジタル署名が添付されているので、発行者以外が改造することは困難である。また払戻許可データには払戻を受領する人もしくは情報処理装置を特定するためのデータが入っていると同時に、第1の情報処理装置が第3の情報処理装置に払戻許可データを送信する前に第1の情報処理装置が有する秘密鍵で暗号化したデジタル署名を添付するので、商品購入者以外が払戻金を不正に受け取ることを防止できる。さらに払戻許可データに使用する払戻金を受領する人もしくは情報処理装置を特定するデータとして、デジタル署名の正当性を証明するために認証局に登録された証書に含まれる人もしくは情報処理装置を特定するためのデータを使用すれば、払戻要求者と払戻を受領する権利を有する人との一致性を容易に検証できる。

【0005】

【発明の実施の形態】以下、本発明に係るオンラインショッピングシステムの実施例を図面を参照しながら説明する。図1は、本発明の全体構成を表わす構成図である。1は商品やサービスを注文する情報処理装置（消費者クライアントと呼ぶ）であり、2は注文を受け付け管理する情報処理装置（受注管理サーバと呼ぶ）であり、3は代金を受け付け管理する情報処理装置（電子マネー決済サーバと呼ぶ）である。4は、前記1から3の情報処理装置を相互に接続しているコンピュータネットワークであり、代表例としてインターネットがある。図2は、消費者クライアント1の構成図である。11は電子マネーを格納する電子マネー格納装置であり、ICカード（スマートカードとも呼ぶ）である場合と、その他の外部記憶装置である場合がある。12はコンピュータネットワークを介して、他の情報処理装置との通信を行う通

信装置であり、電子マネー、注文データ、請求書データ、領収書データなどを送受信するために使用する。13は、プログラムや各種データを記憶する記憶装置であり、デジタル署名を行うための秘密鍵も記憶される。14は、注文データ、請求書データ、領収書データなどを表示するための表示装置である。15は、注文データなどを入力するための入力装置である。16はプログラムを制御するための装置で、デジタル署名を作成、検証したり、入出力を制御したり、通信を制御したり、実行順序を制御する。図3は、受注管理サーバ2の構成図である。21はプログラムや注文データや顧客データなどを記憶する記憶装置であり、デジタル署名に使用する秘密鍵も記憶される。22は他の情報処理装置と通信するための通信装置であり、注文データ、請求書データ、領収書データなどを送受信するために使用する。23は各種データを入力するための入力装置であり、24は各種データを表示するための表示装置である。入力装置23および表示装置24はなくてもよい。25はプログラムを制御するための装置であり、デジタル署名を作成、検証したり、入出力を制御したり、通信を制御したり、実行順序を制御する。図4は、電子マネー決済サーバ3の構成図である。31は電子マネーを格納するための装置であり、電子マネー格納装置11と同様に、ICカードである場合とそれ以外の外部記憶装置である場合がある。32は他の情報処理装置と通信するための通信装置であり、電子マネー、請求書データ、領収書データなどを送受信するために使用する。33はプログラムや各種データを記憶する記憶装置であり、デジタル署名を行うための秘密鍵も記憶される。34は各種データを入力するための入力装置であり、35は各種データを表示するための表示装置である。表示装置34および入力装置35はなくてもよい。以下、本発明のオンラインショッピングシステムで、商品もしくはサービスを購入する場合（購入プロセスとも呼ぶ）と、払戻の場合（払戻プロセスとも呼ぶ）の2つの実施例について説明する。

（1）商品もしくはサービスを購入する場合（購入プロセス）

図5は購入プロセスにおけるメッセージ、請求書データ51、領収書データ53の流れを示すフロー図である。110から220はそれぞれ情報処理装置間で送受信されるメッセージを表わす。請求書データ51に記されている「M」は受注管理サーバ2によってデジタル署名されたことを示す。52は代金受取要求メッセージ150に消費者クライアント1によって添付されたデジタル署名である。領収書データ53に記されている「P」は電子マネー決済サーバ3によってデジタル署名されたことを示す。請求書データ51に記されている「C」52は消費者クライアント1によってデジタル署名されたことを表わす。

【0006】図6は請求書データ51のデータ構造図、

図7は領収書データ53のデータ構造図である。これらのデータ項目は例であり、これ以外のデータ項目が使用されてもよい。デジタル署名は、署名の対象となるデータのハッシュ値を計算し、ハッシュ値に秘密鍵で暗号化したものである。ハッシュ値を算出するために使用されるハッシュ関数にはSHA-1やMD5などのアルゴリズムがある。また秘密鍵で暗号化する方法にはRSAなどの非対称暗号アルゴリズムを使用する。またデジタル署名を検証するためには、秘密鍵と対になっている公開鍵でデジタル署名を復号化したデータと署名の対象となっている平文データのハッシュ値を計算したデータが一致するかどうかをチェックする。55はデータブロック54のハッシュ値に受注管理サーバ2が有する秘密鍵で暗号化したデジタル署名である。58はデータブロック57のハッシュ値に電子マネー決済サーバ3が有する秘密鍵で暗号化したデジタル署名である。図8は消費者クライアント1の処理手順を表わすフロー図である。図9は受注管理サーバ2の処理手順を表わすフロー図である。図10は電子マネー決済サーバ3の処理手順を表わすフロー図である。図11と図12は受注管理サーバ2の記憶装置21に記憶されている注文データ61、62である。図13は電子マネー決済サーバ3の記憶装置33に記憶されている決済データ63である。以下、図5、8、9、及び10を用いて、購入プロセスの処理手順を説明する。消費者クライアント1で注文データが入力されると（ステップ310）、取引相手を認証するために注文準備要求メッセージ110を受注管理サーバ2に送信し、受注管理サーバ2はメッセージを受信すると（ステップ510）、消費者クライアント1に認証用証書を含む注文準備応答メッセージ120を送信する（ステップ520）。消費者クライアント1は、証書を使用して相手認証を行なうと（ステップ320）、受注管理サーバ2に注文データを含む注文要求メッセージ130を送信する（ステップ330）。図14に消費者クライアント1の表示装置に表示される注文データ画面の例を示す。受注管理サーバ2がメッセージ130を受信すると（ステップ530）、注文データを記憶装置21に格納して（ステップ540）、請求書データ51を作成し（ステップ550）、消費者クライアント1に支払要求メッセージ140を送信する（ステップ560）。図15は消費者クライアント1の表示装置に表示される請求書データ画面72である。支払要求メッセージ140を受信したときに、画面72を表示してもよい。消費者クライアント1がメッセージ140を受信すると（ステップ340）、電子マネー決済サーバ3に請求書データ51を含む代金受取要求メッセージ150にデジタル署名52を添付して送信する（ステップ350）。電子マネーサーバ3が前記メッセージ150を受信したら（ステップ710）、請求書データ51とデジタル署名52の有効性をチェックして（ステップ720）、有効

である場合には(ステップ730)、消費者クライアント1に送金開始許可を含む代金受取応答メッセージ160を送信する(ステップ740)。また請求書データ51およびデジタル署名52が有効でない場合には処理を終了する。ステップ730で有効性をチェックする方法には、請求書データ51に受注管理サーバ2のデジタル署名55が添付されているかどうか、請求書データ51に含まれる支払者を特定するためのデータ(支払者IDなど)とデジタル署名52を署名した者が同一であるかどうかをチェックする方法などがある。消費者クライアント1が代金受取応答メッセージ160を受信し(ステップ360)、メッセージ160の中に送金許可を示すデータが含まれている場合(ステップ370)、電子マネー決済サーバ3に電子マネー170を送信する(ステップ380)。電子マネー決済サーバ3が電子マネー170を受信したら(ステップ750)、記憶装置33の決済データ63を更新し、電子マネーを受領したことを示すメッセージ180を消費者クライアント1に送信する(ステップ760)。消費者クライアント1がメッセージ180を受信したら(ステップ390)、電子マネー決済サーバ3に領収書データを要求するメッセージ190を送信する(ステップ400)。電子マネー決済サーバ3がメッセージ190を受信したら(ステップ770)、領収書データ53を作成し(ステップ780)、消費者クライアント1に領収書データ53を含む領収書応答メッセージ200を送信する(ステップ790)。消費者クライアント1がメッセージ200を受信したら(ステップ410)、領収書データ53を含む支払応答メッセージ210を受注管理サーバ2に送信する(ステップ420)。図16は消費者クライアント1の表示装置に表示される領収書データ画面73である。領収書応答メッセージ200を受信したときに、画面73を表示してもよい。受注管理サーバ2がメッセージ210を受信したら(ステップ570)、領収書データ53の有効性をチェックして(ステップ580)、領収書データ53が有効である場合には(ステップ590)、記憶装置21に格納されている注文データ61を更新して(600)、消費者クライアント1に注文完了を示す注文応答メッセージ220を送信する(ステップ610)。領収書データ53が有効でない場合には(ステップ590)、消費者クライアント1に注文失敗を示す注文応答メッセージ220を送信する(ステップ620)。ステップ580の有効性をチェックする方法には、領収書データ53に請求書データ51で指定した支払先のデジタル署名が添付されているかどうか、領収書データ53に含まれる受賞金額に関するデータが代金の金額と一致するかどうかなどをチェックする方法がある。消費者クライアント1が受注管理サーバ2から注文応答メッセージ220を受信すると(ステップ430)、購入プロセスが完了する。以上の処理により、消費者クライアント

1、受注管理サーバ2、電子マネー決済サーバ3がそれぞれコンピュータネットワーク4に接続されている場合に安全に取引を行うことが可能になる。また請求書データ51や領収書データ53は、後日取引上の問題が起こった場合に取引内容や決済完了状態を示す証拠として使用することができる。さらに前記ステップ720により、電子マネー決済サーバ3への不正アクセスを防止することができる。

(2) 払戻の場合(払戻プロセス)

図17は払戻プロセスにおけるメッセージ、払戻許可書データ(払戻許可データとも呼ぶ)81、払戻領収書83の流れを示すフロー図である。1110から1220はそれぞれ情報処理装置間で送受信されるメッセージを表わす。払戻許可書データ81に記されている「M」は受注管理サーバ2によってデジタル署名されたことを表わす。82は払戻金送金要求メッセージ1150に消費者クライアント1によって添付されたデジタル署名である。払戻領収書83に記されている「C」は消費者クライアント1によってデジタル署名されたことを表わす。図18は払戻許可書データ81のデータ構造図、図19は払戻領収書83のデータ構造図である。これらのデータ項目は例であり、他のデータ項目が使用されてもよい。85はデータブロック84のハッシュ値に受注管理サーバ2が有する秘密鍵で暗号化されたデジタル署名である。88はデータブロック87のハッシュ値に消費者クライアント1が有する秘密鍵で暗号化されたデジタル署名である。図20は消費者クライアント1の処理手順を表わすフロー図である。図21と図22は受注管理サーバ2の処理手順を表わすフロー図である。図23は電子マネー決済サーバ3の処理手順を表わすフロー図である。以下、図17、20、21、22、及び23を用いて、払戻プロセスの処理手順を説明する。消費者クライアント1で払戻を行うために必要なデータを入力装置15を用いて入力されると(ステップ1310)、受注管理サーバ2に払戻要求メッセージ1110を送信する(ステップ1320)。図24は前記消費者クライアント1の表示装置14に表示される払戻要求するための画面91である。受注管理サーバ2が前記メッセージ1110を受信したら(ステップ1510)、メッセージで指定された取引IDが払戻可能かどうかをチェックし(ステップ1520)、可能であるならば電子マネー決済サーバ3に払戻準備要求メッセージ1120を送信する(ステップ1530)。電子マネー決済サーバ3がメッセージ1120を受信したら(ステップ1710)、記憶装置33に記憶されている決済データ63を「払戻中」に更新して(ステップ1720)。受注管理サーバ2に準備完了を示す払戻準備応答メッセージ1130を送信する(ステップ1730)。受注管理サーバ2が応答メッセージ1130を受信したら(ステップ1540)、記憶装置21の注文データ61を「払戻中」に更

新し(ステップ1550)、払戻許可書データ81を作成して(ステップ1560)、消費者クライアント1に払戻許可書データ81を含む払戻応答メッセージ1140を送信する(ステップ1570)。消費者クライアント1が応答メッセージ1140を受信したら(ステップ1330)、応答メッセージ1140に含まれる払戻許可書データ81を含む払戻金送金要求メッセージ1150に消費者クライアント1が有する秘密鍵で暗号化したデジタル署名82を添付して電子マネー決済サーバ3に送信する(ステップ1340)。図25は消費者クライアント1の表示装置14に表示される払戻許可書データの画面92である。払戻応答メッセージ1140を受信したときに画面92を表示してもよい。電子マネー決済サーバ3が要求メッセージ1150を受信したら(ステップ1740)、払戻許可書データ81とデジタル署名82を用いて払戻が可能かどうかチェックする(ステップ1750)。この場合のチェック方法として、払戻許可書データ81に受注管理サーバ2のデジタル署名が添付されているか、払戻許可書データ81で指定される払戻受領者がデジタル署名82を署名した者と一致するかなどをチェックする方法がある。ステップ1750の結果が有効である場合には(ステップ1760)、消費者クライアント1に払戻許可を示すデータを含む払戻金送金応答メッセージ1160を送信する(ステップ1770)。ステップ1750の結果が無効である場合には(ステップ1760)、払戻不可を示すデータを含む払戻金送金応答メッセージ1160を消費者クライアント1に送信する(ステップ1850)。消費者クライアント1が応答メッセージ1160を受信し(ステップ1350)、メッセージ1160に払戻許可を示すデータが含まれている場合には(ステップ1360)、電子マネー決済サーバ3に電子マネー送金要求を示すメッセージ1170を送信する(ステップ1370)。ステップ1360でメッセージ1160に払戻不可を示すデータが含まれている場合には処理を終了する。電子マネー決済サーバ3がメッセージ1170を受信したら(ステップ1780)、消費者クライアント1に電子マネー1180を送金する(ステップ1790)。消費者クライアント1が電子マネー1180を受信したら(ステップ1380)、払戻領収書データ83を作成して(ステップ1390)、領収書データ83を含む払戻領収書送信メッセージ1190を電子マネー決済サーバ3に送信する(ステップ1400)。電子マネー決済サーバ3がメッセージ1190を受信したら(ステップ1800)、記憶装置33に記憶されている決済データ63を「払戻完了」に更新して(ステップ1810)、払戻領収書応答メッセージ1200を消費者クライアント1に送信する(ステップ1820)。消費者クライアント1が応答メッセージ1200を受信したら(ステップ1410)、処理を終了する。受注管理サーバ2は所定の時間が経過

したら電子マネー決済サーバ3に払戻状態要求メッセージ1210を送信する(ステップ1610)。電子マネー決済サーバ3が要求メッセージ1210を受信したら(ステップ1830)、受注管理サーバ2に払戻完了状態を含む払戻状態応答メッセージ1220を送信する(ステップ1840)。このとき既に払戻が完了している場合には、応答メッセージ1220で消費者クライアント1から受け取った払戻領収書83を送信してもよい。受注管理サーバ2は、応答メッセージ1220を受信したら(ステップ1620)、記憶装置21に記憶されている注文データ61を「払戻完了」に更新して(ステップ1630)、処理を終了する。以上の処理により、消費者クライアント1、受注管理サーバ2、電子マネー決済サーバ3がそれぞれコンピュータネットワーク4に接続されている場合に安全に電子マネーを用いて払い戻しすることが可能になる。また払戻許可書データ81や払戻領収書データ83は、後日払戻に関する問題が起こった場合に払戻内容や払戻完了状態を示す証拠として使用することができる。さらにステップ1750により、電子マネー決済サーバ3への不正アクセスを防止することができる。図8又は20に示した処理を実行するプログラムをフロッピーディスクなどの可搬記憶媒体に格納し、これを消費者クライアント1の記憶部13に読み込んで実行することも可能である。受注管理サーバ2、及び電子マネー決済サーバ3についても同様である。

【0007】

【発明の効果】オープンネットワーク上で電子マネーを使用してショッピングを行ない、後日問題が発生した場合に取引関与者が取引内容や決済状態を証明することが可能になる。また第三者が不正に取引に介入することを防止できる。さらにオープンネットワーク上で電子マネーを使用して代金の払戻を安全に行うことができる。

【図面の簡単な説明】

【図1】本発明の全体構成を表わす構成図である。

【図2】消費者クライアント1の構成図である。

【図3】受注管理サーバ2の構成図である。

【図4】電子マネー決済サーバ3の構成図である。

【図5】購入プロセスのメッセージ、請求書データ51、領収書データ53のフロー図である。

【図6】請求書データ51のデータ構造図である。

【図7】領収書データ53のデータ構造図である。

【図8】購入プロセスにおける消費者クライアント1の処理フロー図である。

【図9】購入プロセスにおける受注管理サーバ2の処理フロー図である。

【図10】購入プロセスにおける電子マネー決済サーバ3の処理フロー図である。

【図11】受注管理サーバ2の記憶装置21に記憶され

ている注文データ構造61である。

【図12】受注管理サーバ2の記憶装置21に記憶されている注文データ構造62である。

【図13】電子マネー決済サーバ3の記憶装置33に記憶されている決済データ構造63である。

【図14】注文データが表示されている消費者クライアント画面71である。

【図15】請求書データ51が表示されている消費者クライアント画面72である。

【図16】領収書データ53が表示されている消費者クライアント画面73である。

【図17】払戻プロセスのメッセージ、払戻許可データ81、払戻領収書データ83のフロー図である。

【図18】払戻許可書データ81のデータ構造図である。

【図19】払戻領収書データ83のデータ構造図である。

【図20】払戻プロセスにおける消費者クライアント1の処理フロー図である。

【図21】払戻プロセスにおける受注管理サーバ2の処理フロー図である。

【図22】払戻プロセスにおける受注管理サーバ2の処理フロー図である。

【図23】払戻プロセスにおける電子マネー決済サーバ3の処理フロー図である。

【図24】払戻要求書データが表示されている消費者クライアント画面91である。

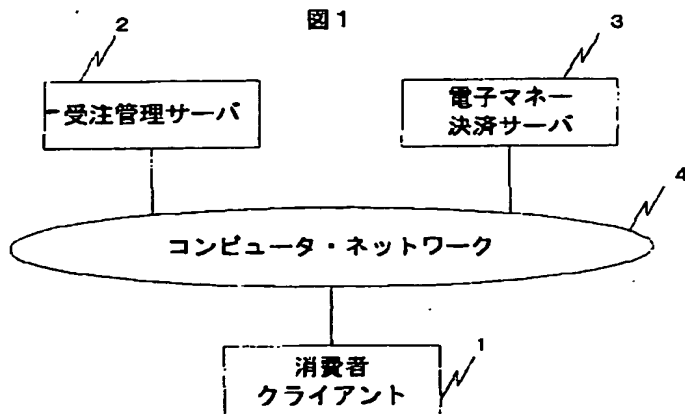
【図25】払戻許可書データ81が表示されている消費者クライアント画面92である。

【符号の説明】

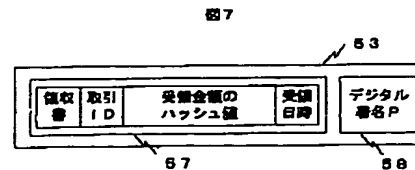
1…消費者クライアント、2…受注管理サーバ、3…電

子マネー決済サーバ、4…コンピュータネットワーク、11から16…消費者クライアントの構成要素、21から25…受注管理サーバの構成要素、31から36…電子マネー決済サーバの構成要素、51…請求書データ、52…消費者クライアント1のデジタル署名、53…領収書データ、54…請求書データの平文データブロック、55…データブロック54に対するデジタル署名、57…領収書データの平文データブロック、58…データブロック57に対するデジタル署名、61、62…受注管理サーバに記憶されている注文データ、63…電子マネー決済サーバに記憶されている決済データ、71…注文データ画面、72…請求書画面、73…領収書画面、81…払戻許可書データ、82…消費者クライアント1のデジタル署名、83…払戻領収書データ、84…払戻許可書データの平文データブロック、85…データブロック84に対するデジタル署名、87…払戻領収書データの平文データブロック、88…データブロック87に対するデジタル署名、91…払戻要求書画面、92…払戻許可書画面、110から220…購入プロセスで使用される通信メッセージ、310から430…購入プロセスにおける消費者クライアント1の処理ステップ、510から610…購入プロセスにおける受注管理サーバ2の処理ステップ、710から790…購入プロセスにおける電子マネー決済サーバ3の処理ステップ、1110から1220…払戻プロセスで使用される通信メッセージ、1310から1410…払戻プロセスにおける消費者クライアント1の処理ステップ、1510から1630…払戻プロセスにおける受注管理サーバ2の処理ステップ、1710から1850…払戻プロセスにおける電子マネー決済サーバ3の処理ステップ

【図1】



【図7】



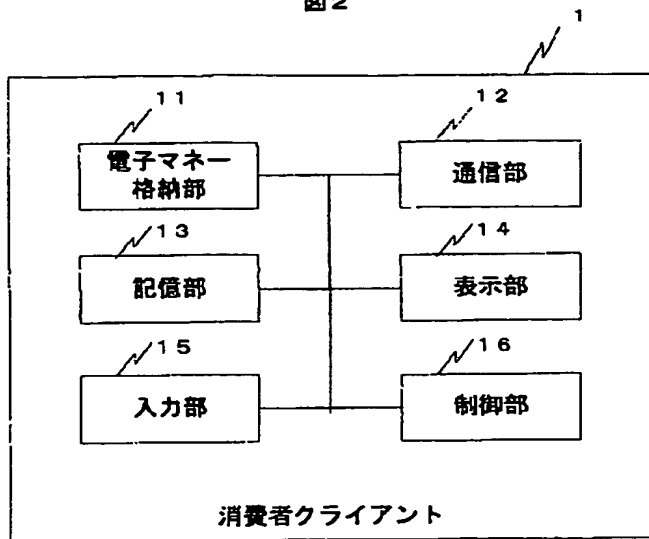
【図11】

図11

取引ID	購入者ID	代金合計	決済方法	決済状態
210181	9821358	5,000	クレジットA	決済完了
210182	8790392	2,600	電子マネー	決済完了
210183	3789817	4,000	電子マネー	承認完了
210184	4789711	1,000	電子マネー	決済完了
210185	1789090	4,000	クレジットB	承認完了
:	:	:	:	:

【図2】

図2



【図12】

図12

取引ID	商品名	個数	単価	金額
210191	商品A	1	1,000	1,000
	商品B	2	2,000	4,000
210192	商品C	1	2,500	2,500
210193	商品A	1	1,000	1,000
	商品C	1	1,500	3,000
210194	商品A	1	1,000	1,000
210195	商品B	2	2,000	4,000
:	:	:	:	:

【図13】

図13

取引ID	購入者ID	小売店ID	代金合計	決済状態
210192	8790392	1230001	2,500	決済完了
210193	3090890	1230001	4,000	決済完了
210194	4789711	1230001	1,000	決済完了
120930	4343280	0090800	2,300	決済完了
230090	1349222	0900202	3,200	決済完了
:	:	:	:	:

【図14】

図14

図14は、注文書の画面表示を示す。画面には以下の情報が表示されている。

商品名称	単価	個数
商品A	1,000	1
商品C	1,500	2

合計金額 4,000円

【図15】

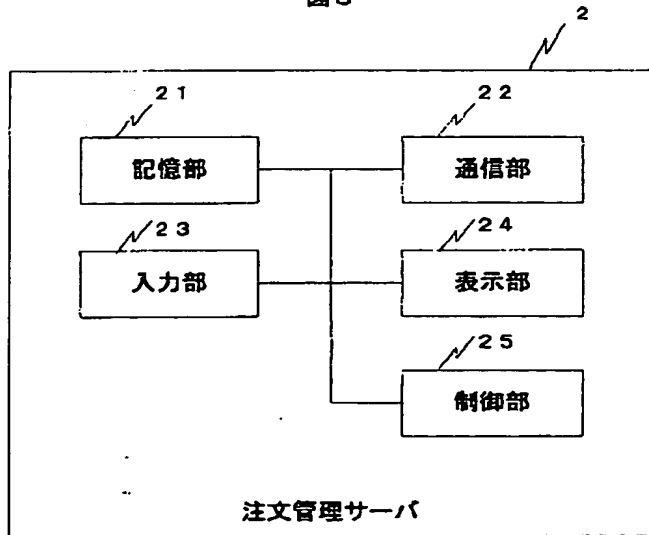
図15

図15は、請求書の画面表示を示す。画面には以下の情報が表示されている。

取引ID	210193
購入者ID	3789817
注文内容	商品A 1個 商品C 2個
支払金額	4,000円
支払方法	電子マネー
小売店名	東京オンライン通販
支払先名	ABC代金回収サービス
支払先アドレス	http://www.abc.com
請求日時	1998.12.8 14:20
支払期限	1998.12.10 17:00

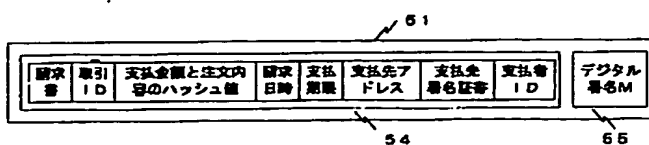
【図3】

図3



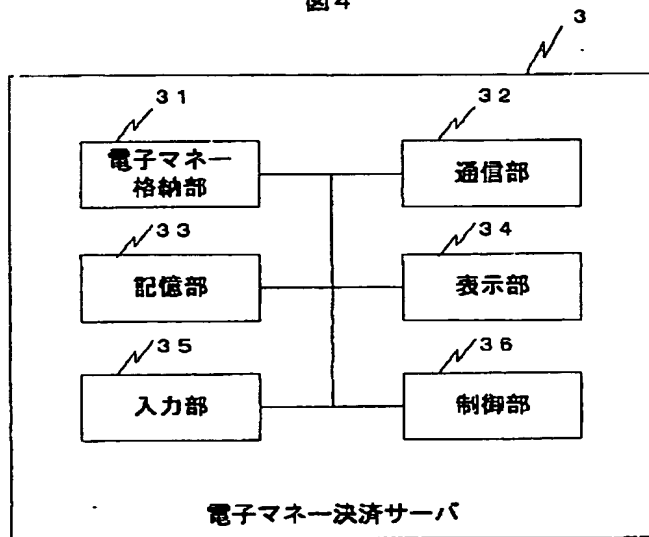
【図6】

図6



【図4】

図4



【図16】

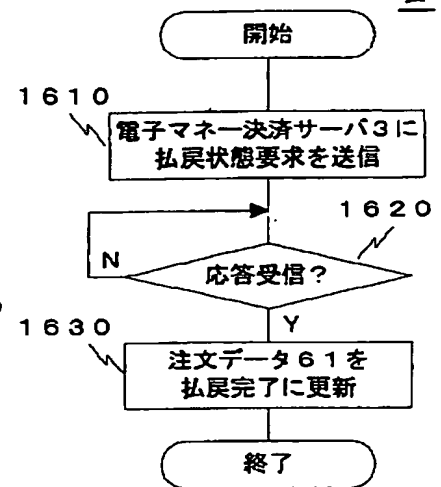
図16

領収書	
取引ID	210163
購入者ID	3789817
領収金額	4,000円
領収方法	電子マネー
小売店名	東京オンライン通販
領収者名	ABC代金徴収サービス
領収日時	1998.12.8 14:20

【図22】

図22

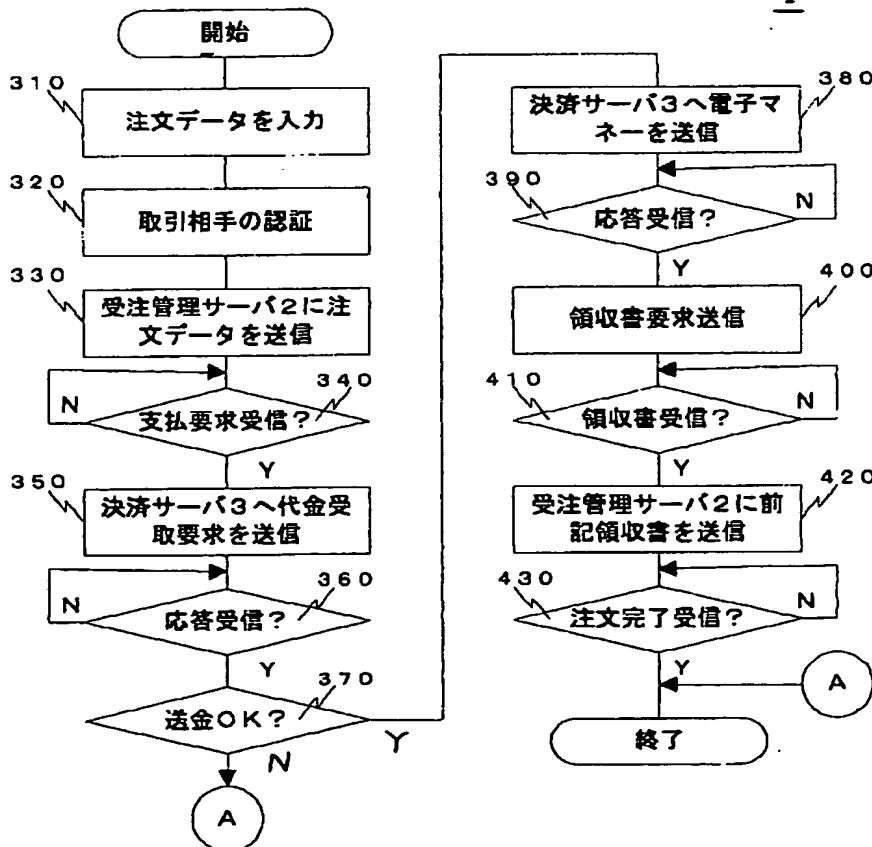
2



【図8】

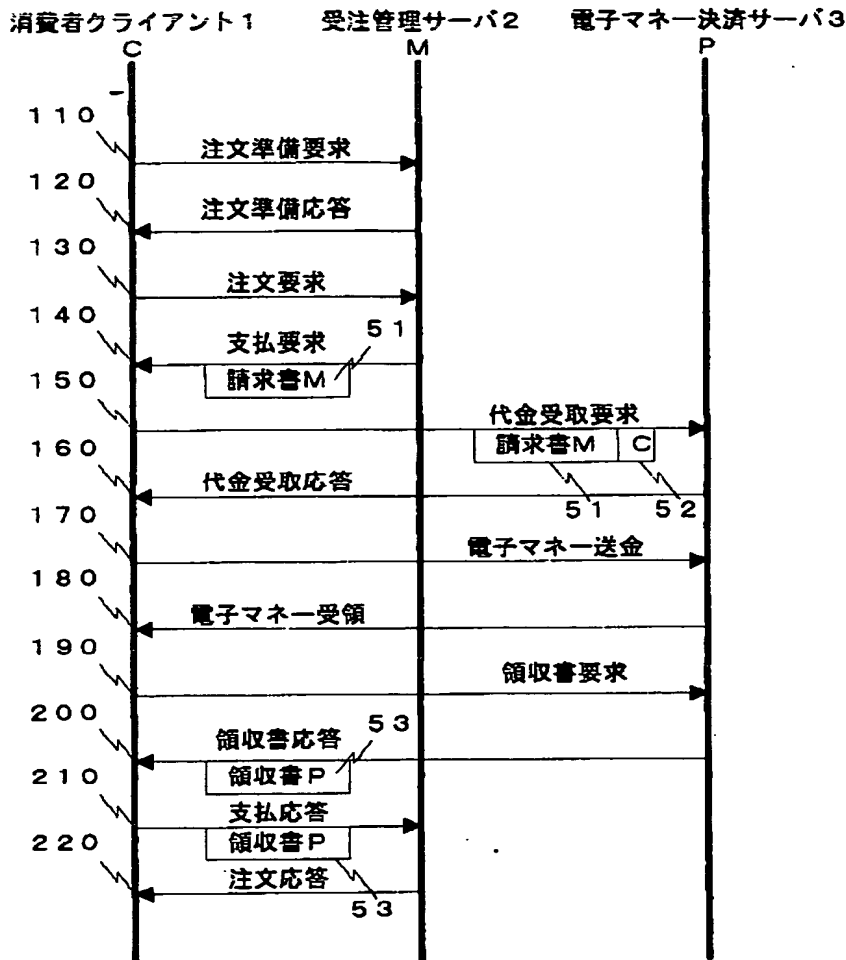
図8

1



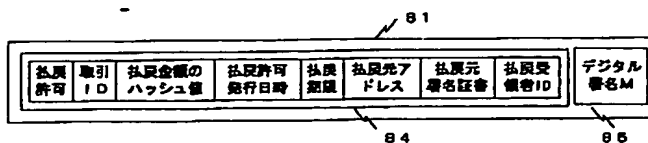
【図5】

図5



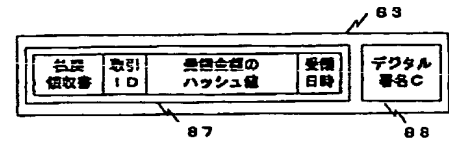
【図18】

図18



【図19】

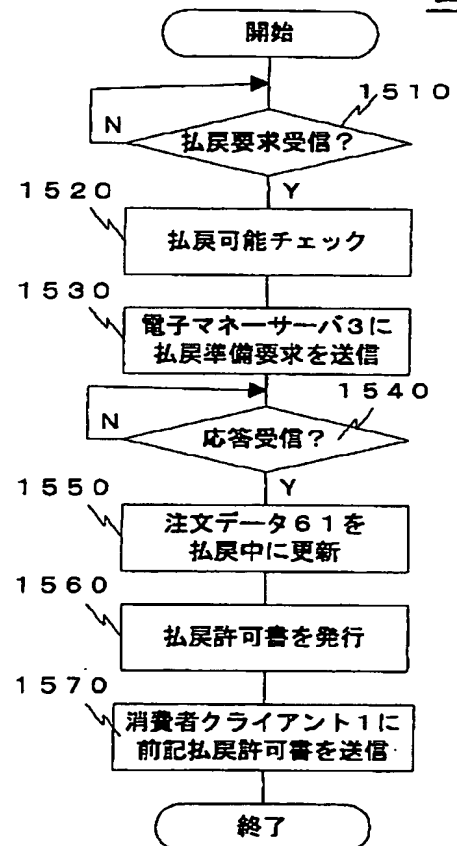
図19



【図21】

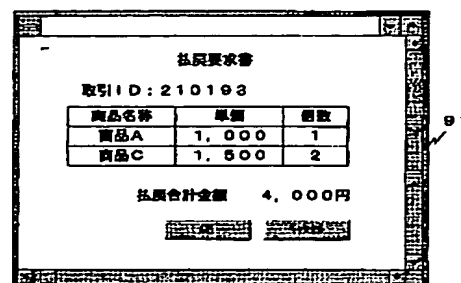
図21

2



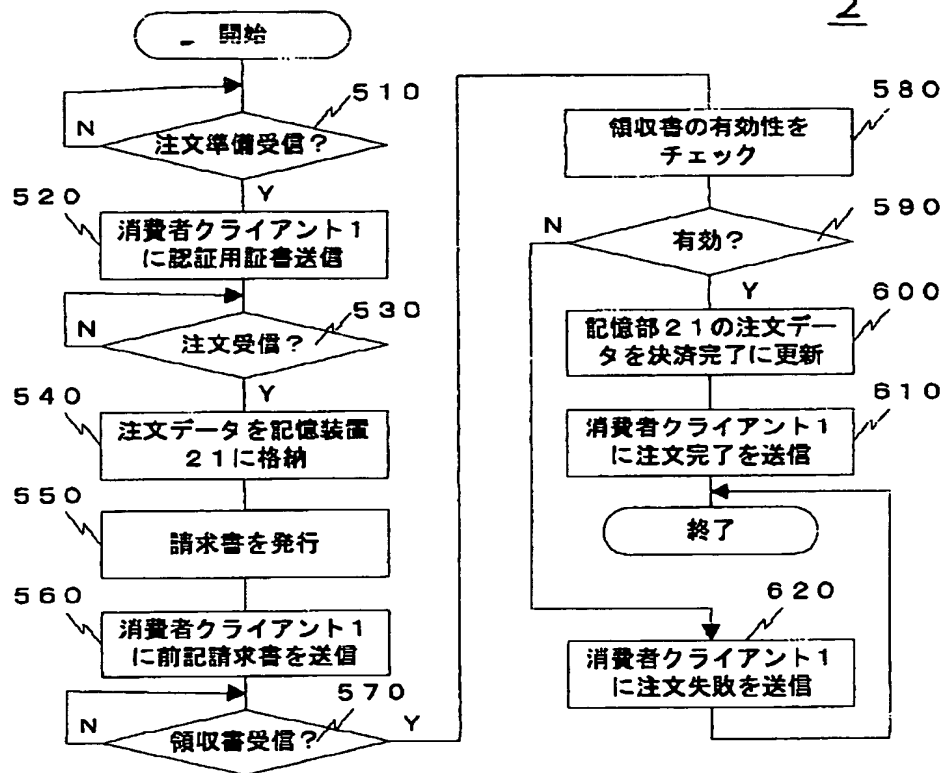
【図24】

図24



【図9】

図9



【図25】

図25

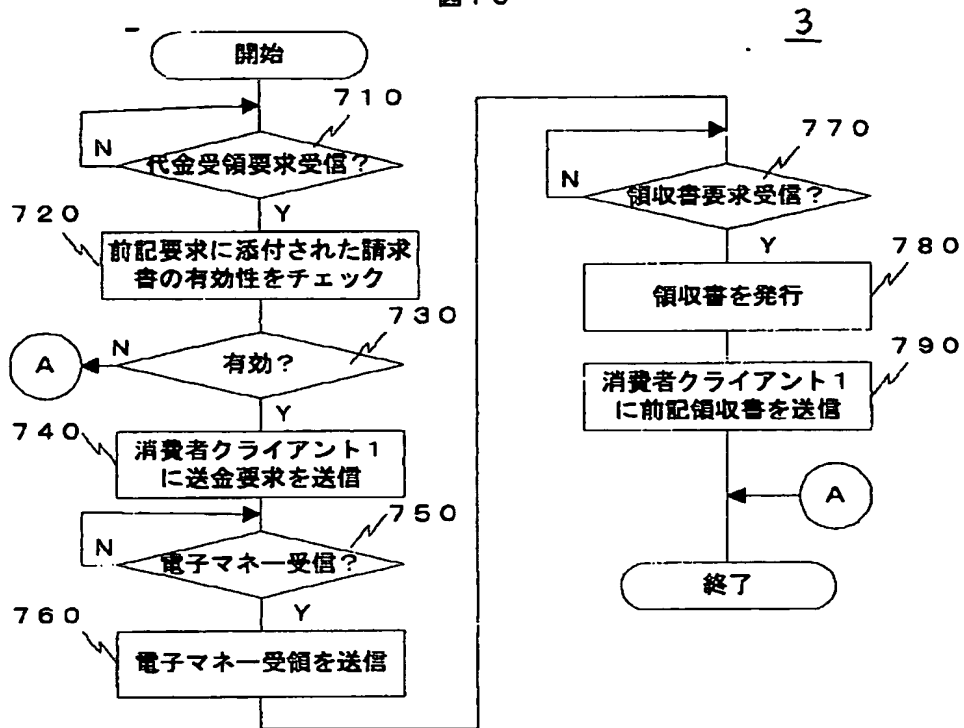
払戻許可書

取引ID	210103
払戻受領者ID	3789817
払戻金額	4,000円
払戻方法	電子マネー
小売店名	東京オンライン通販
払戻元名	ABC代金振込サービス
払戻元アドレス	http://www.abc.com
払戻許可日時	1999.12.12 18:10
払戻期限	1999.12.15 18:10

92

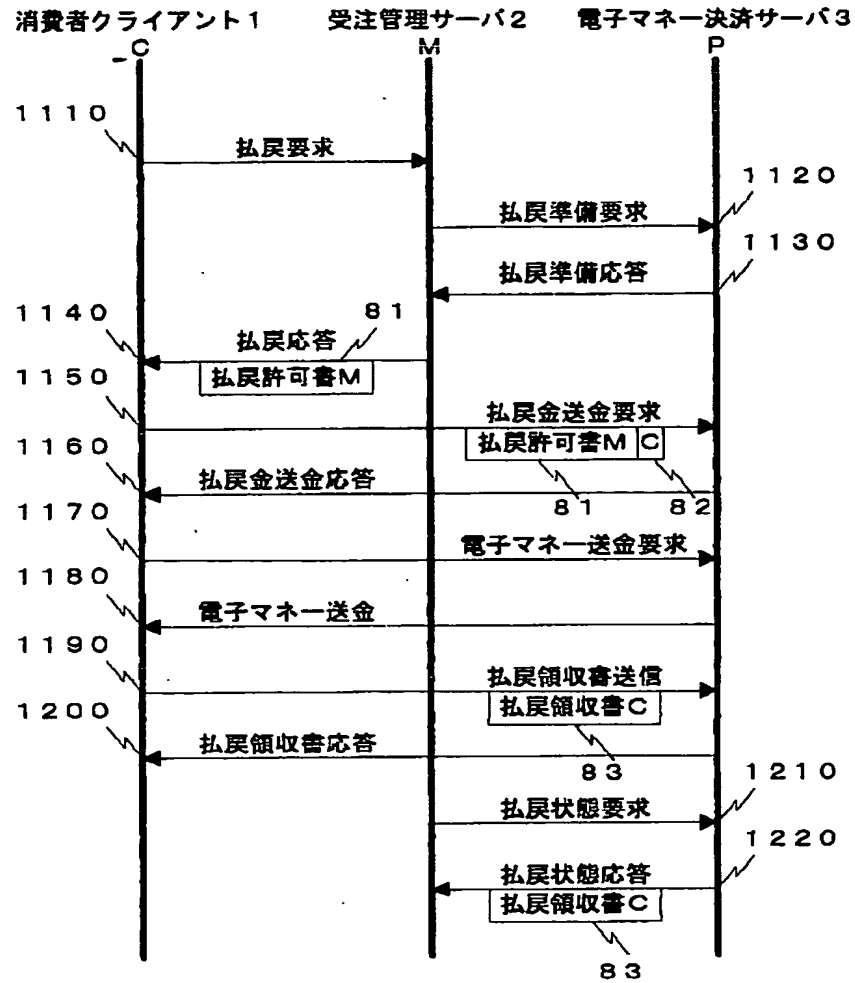
【図10】

図10



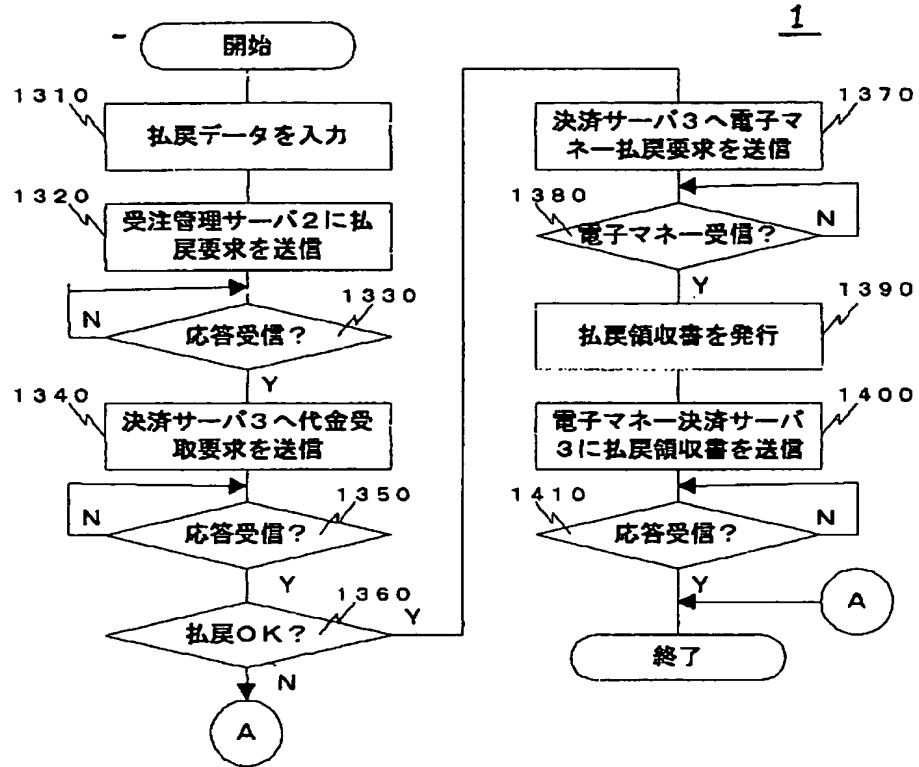
【図17】

図17



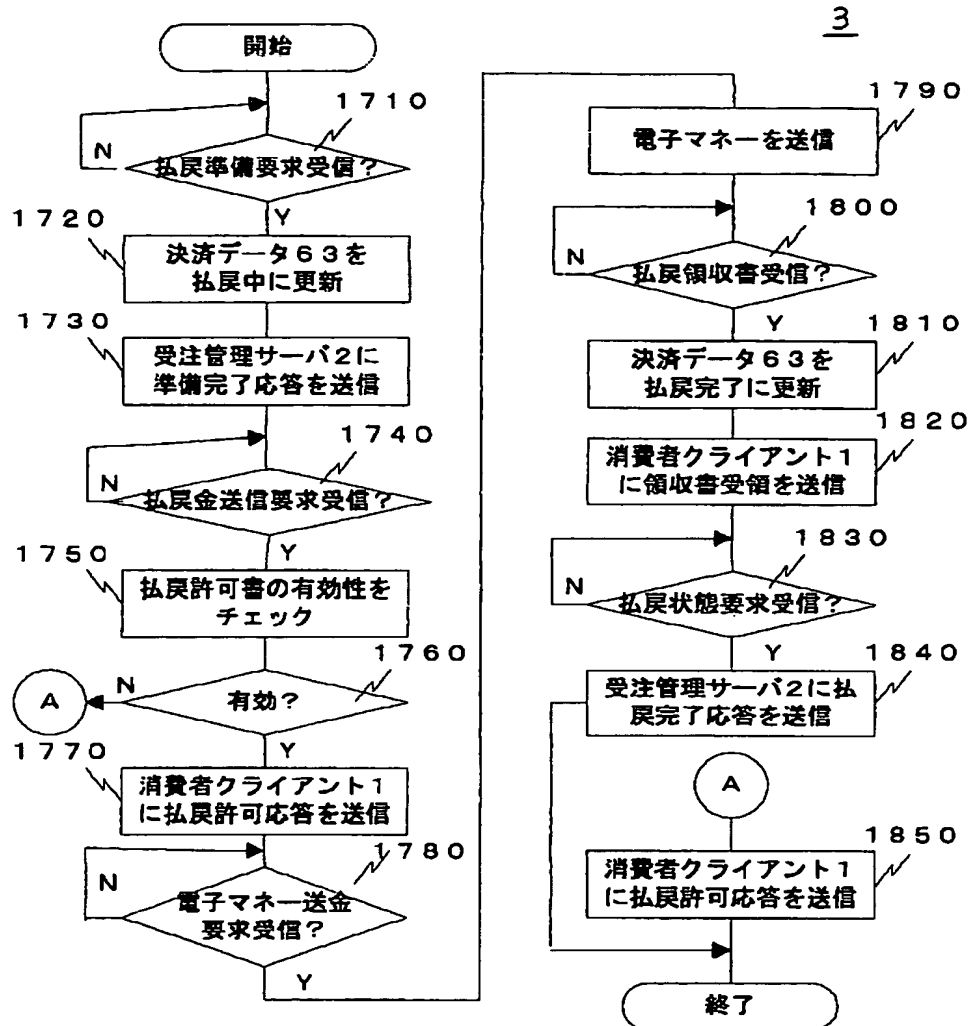
【図20】

図20



【図23】

図23



フロントページの続き

(72)発明者 伊藤 淳史
 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72)発明者 川連 嘉晃
 神奈川県横浜市都筑区加賀原二丁目2番 株式会社日立製作所ビジネスシステム開発センタ内

(72)発明者 寺村 健
 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72)発明者 富山 朋哉
 神奈川県横浜市都筑区加賀原二丁目2番 株式会社日立製作所ビジネスシステム開発センタ内